2015R00078/DS

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Criminal No. 15- 626 (WJM)
	:	
v.	:	18 U.S.C. § 371
	:	18 U.S.C. § 1349
TIMOTHY LIVINGSTON,	:	
a/k/a "Mark Loyd,"	:	
TOMASZ CHMIELARZ, and	:	
DEVIN McARTHUR	:	

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

COUNT ONE
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

1. At all times relevant to this Indictment:

Relevant Individuals and Entities

a. Defendant TIMOTHY LIVINGSTON, a/k/a "Mark Loyd," resided in or around Fort Lauderdale, Florida, and was the sole owner of A Whole Lot of Nothing LLC ("AWLN"), a company that sent unsolicited emails in bulk (or "spam") on behalf of its customers for a fee. Defendant LIVINGSTON was the organizer and leader of the computer hacking and illegal spamming schemes described herein.

b. Defendant TOMASZ CHMIELARZ resided in or around Clifton, New Jersey, and was a computer programmer. Among other things, defendant CHMIELARZ authored the hacking tools and other programs used to facilitate the computer hacking and illegal spamming schemes described herein.

c. Defendant DEVIN McARTHUR resided in or around Ellicott City, Maryland. Among other things, defendant McARTHUR worked at Corporate Victim #4 and used his access to Corporate Victim #4's computer networks to install hacking tools on them in order to facilitate the exfiltration of data from Corporate Victim #4's networks.

d. "Corporate Victim #1" was a telecommunications company headquartered in New York that, among other things, provided email services to its customers.

e. "Corporate Victim #2" was a technology and consulting company headquartered in New York.

f. "Corporate Victim #3" was a company that provided credit monitoring services and was headquartered in Texas.

g. "Corporate Victim #4" was a telecommunications company headquartered in Pennsylvania.

Relevant Terms

h. A "botnet" was a collection of computers infected with malware without the users' authorization and controlled by a hacker using a central "command and control" computer.

i. An "Internet Protocol address," or "IP address," was a unique numeric address used by a computer on the internet. Every computer connected to the internet was assigned an IP address.

j. "Proxy servers" were computer systems or applications that acted as intermediaries for requests from computer users seeking resources from

other servers. Proxy servers had a large variety of potential uses, including hiding one's true IP address from others, thereby remaining anonymous, and evading anti-spam filters and other spam-blocking techniques.

k. A "remote administration tool" was a piece of software that allowed a remote operator to control a computer system as if he had physical access to that system.

Overview

2. From in or about January 2012 through in or about July 2015, defendants LIVINGSTON, CHMIELARZ, and McARTHUR, together with others: (1) hacked into the computer networks of Corporate Victim #3 and Corporate Victim #4 to steal the personally identifiable information ("PII") of tens of millions of individuals; (2) compromised the personal email accounts of numerous individuals, including customers of Corporate Victim #1; (3) compromised a number of websites, including Corporate Victim #2's, in order to use it in their illegal spamming activities; and (4) used stolen PII as well as compromised corporate computer networks and email accounts to send illegal spam on behalf of others for a fee. In total, the scheme generated more than $2 million in illegal profits.

The Illegal Spamming Infrastructure

3. Beginning as early as 2011, defendant LIVINGSTON together with others operated AWLN — a business that specialized in sending spam on behalf of its clients. LIVINGSTON's clients included legitimate businesses, such as

insurance companies that wished to send bulk emails to advertise their businesses, as well as illegal entities, such as online pharmacies that sold narcotics without prescriptions. Typically, defendant LIVINGSTON charged between $5 and $9 for each spam email that resulted in a completed transaction for a client.

4. During the period of the schemes described herein, many internet service providers utilized spam filters designed to prevent spam from reaching their customers' email accounts. Beginning in or about January 2012, however, defendant LIVINGSTON solicited defendant CHMIELARZ to write computer programs to send spam in a manner that would conceal the true origin of the email and bypass spam filters.

5. Also beginning in or around January 2012, defendants LIVINGSTON and CHMIELARZ started using proxy servers to send out spam messages using botnets to hide the true origin of the spam, help them remain anonymous, and to evade anti-spam filters and other spam blocking techniques. Defendant LIVINGSTON also registered certain websites used in the spam campaigns in the name of his alias, "Mark Lloyd," to avoid detection.

6. In addition, defendants LIVINGSTON and CHMIELARZ also hacked into the email accounts of individuals and compromised and seized control of the mail servers of certain of the Corporate Victims to further their spam campaigns.

Corporate Victim #1's Customer Accounts

7. For example, defendants LIVINGSTON and CHMIELARZ created custom software designed to hack into the email accounts of Corporate Victim #1's customers (the "Email Account Software"). Once the Email Account Software gained access to a Corporate Victim #1 user's account, it then created sub-accounts on the account and used those sub-accounts to send out spam. To avoid detection, defendants LIVINGSTON and CHMIELARZ programmed the Email Account Software to access the mail server of Corporate Victim #1 through proxy servers to obscure their true identities. In effect, this allowed defendants LIVINGSTON and CHMIELARZ to send out massive amounts of email spam without identifying themselves as the true senders, and instead using Corporate Victim #1's mail servers and Corporate Victim #1's customer accounts.

8. On or about October 24, 2012, defendant LIVINGSTON sent defendant CHMIELARZ the username and password for several email accounts hosted by Corporate Victim #1 so that defendant CHMIELARZ could use them to test the Email Account Software.

9. On or about July 23, 2015, law enforcement seized defendant LIVINGSTON's computer (the "Livingston Computer"). A subsequent search of that computer revealed that defendant LIVINGSTON maintained on that computer a list of tens of thousands of usernames and passwords for email accounts hosted by Corporate Victim #1.

Use of Corporate Victim #2's Website in Furtherance of the Scheme

10. Defendants LIVINGSTON and CHMIELARZ also created custom software that leveraged vulnerabilities in the websites of a number of corporations, including Corporate Victim #2 (the "Web Form Software"). The Web Form Software allowed defendants LIVINGSTON and CHMIELARZ to use Corporate Victim #2's email servers to send out spam that appeared to be from Corporate Victim #2. Specifically, the conspirators used the Web Form Software to enter commands into the user submitted forms portion of Corporate Victim #2's websites. Those commands essentially directed Corporate Victim #2's mail servers to send specific spam to individuals as directed by the conspirators; to its recipients, the spam appeared to originate from Corporate Victim #2.

11. To further avoid detection, defendants LIVINGSTON and CHMIELARZ programmed the Web Form Software to access Corporate Victim #2's networks using proxy servers to obscure their true identities. In effect, this allowed the conspirators to send out massive amounts of spam without identifying themselves as the true senders.

12. In an online chat dated on or about March 15, 2013, defendants LIVINGSTON and CHMIELARZ discussed creating a modified version of the Web Form Software to target the website of Corporate Victim #2. Subsequently, on or about March 16, 2013, defendant CHMIELARZ sent defendant LIVINGSTON what he purported to be a modified version of the Web Form Software to target the website of Corporate Victim #2. Shortly thereafter, on or about March 22,

2013, Corporate Victim #2 was notified by Google that their mail server had been compromised and was sending out spam.

The Computer Hacking Victims

13. Defendants LIVINGSTON, CHMIELARZ, and McARTHUR also worked together to steal the confidential business information of the Corporate Victims, including databases containing the PII of millions of Americans, so that they could use that information in spam campaigns.

The Compromise of Corporate Victim #3's Network

14. In or around May of 2013, defendants LIVINGSTON and CHMIELARZ discussed stealing confidential business information from Corporate Victim #3. Specifically, in an online chat dated on or about May 9, 2013, defendant LIVINGSTON told defendant CHMIELARZ, "here is the site I need scrapped [*sic*]," and provided defendant CHMIELARZ with an address for Corporate Victim #3's website and the login credentials for an employee of Corporate Victim #3. "Scraping" is a technique employed to extract large amount of data from websites.

15. Thereafter, in an online chat dated on or about May 10, 2013, defendant LIVINGSTON told defendant CHMIELARZ that the database they were going to steal from Corporate Victim #3 contained approximately 10 million records. Defendant LIVINGSTON subsequently paid defendant CHMIELARZ to write a computer program to steal the database from Corporate Victim #3.

16. In another online chat dated on or about May 10, 2013, defendant LIVINGSTON told defendant CHMIELARZ that the program he wrote was working and that it had downloaded 200,000 records so far.

The Compromise of Corporate Victim #4's Network

17. From in or about February 2014 through in or about February 2015, defendant McARTHUR was employed as a sales representative at Corporate Victim #4. In a series of online chats dated in or about August 2014, defendants LIVINGSTON, CHMIELARZ, and McARTHUR discussed using defendant McARTHUR's position at Corporate Victim #4 to steal confidential business information from Corporate Victim #4, including the PII of millions of Corporate Victim #4's customers.

18. On or about August 11, 2014, defendant McARTHUR provided defendant LIVINGSTON with access to a remote administration tool on a computer with access to the computer network of Corporate Victim #4 without authorization from his employer. Thereafter, on or about August 15, 2014, defendant McARTHUR gave defendants LIVINGSTON and CHMIELARZ access to Corporate Victim #4's computer network using the remote administration tool for the purpose of stealing the names, addresses, phone numbers, and email addresses of potential customers, current customers, and former customers of Corporate Victim #4 so that defendants LIVINGSTON, CHMIELARZ, McARTHUR, and others could use that information to send spam to those individuals.

19. In an online chat dated on or about August 15, 2014, defendant LIVINGSTON told defendant CHMIELARZ that he estimated that Corporate Victim #4's database had records for approximately 50 million people; defendant LIVINGSTON also discussed the technical challenges associated with stealing such a large volume of data from Corporate Victim #4.

20. On or about August 15, 2014, defendant LIVINGSTON agreed to pay defendant CHMIELARZ to design a computer program to steal the database from Corporate Victim #4 using the remote administration tool that defendant McARTHUR had installed. Also, on or about August 15, 2014, defendant LIVINGSTON provided defendant CHMIELARZ with defendant McARTHUR's network username and password, which allowed defendant CHMIELARZ to access the database of Corporate Victim #4.

21. In an online chat dated on or about September 3, 2014, defendants LIVINGSTON and McARTHUR discussed the contents of the database that they had stolen from Corporate Victim #4. In that conversation, defendant McARTHUR estimated that they had succeeded in stealing over 24.5 million records from Corporate Victim #4. Defendants LIVINGSTON and McARTHUR further discussed whether they should sell the database, but ultimately agreed to use it first to send out spam.

22. As referenced in paragraph 9, on or about July 23, 2015, law enforcement seized the Livingston Computer. A subsequent search of that computer revealed that defendant LIVINGSTON retained a portion of the

database stolen from Corporate Victim #4 containing more than approximately 7 million records.

23. Ultimately, defendants LIVINGSTON, CHMIELARZ and MACARTHUR earned more than $2 million dollars selling spamming services using the means and methods discussed above.

The Conspiracy

24. From at least as early as in or about February 2011 through in or about September 2015, in Passaic County, in the District of New Jersey, and elsewhere, defendants

TIMOTHY LIVINGSTON,
a/k/a "Mark Loyd,"
TOMASZ CHMIELARZ, and
DEVIN McARTHUR

did knowingly and intentionally conspire and agree with each other and others to commit an offense against the United States, namely, to intentionally access a computer without authorization and to exceed authorized access to a computer, and thereby obtain information from a protected computer for the purposes of commercial advantage and private financial gain, where the value of the information obtained exceeded $5,000, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), and 1030(c)(2)(B)(iii).

Object of the Conspiracy

25. The object of the conspiracy was for defendant LIVINGSTON, defendant CHMIELARZ, defendant McARTHUR, and others to enrich themselves

by: (1) hacking into the computer networks of Corporate Victim #3 and Corporate Victim #4 to steal the PII of tens of millions of individuals; (2) compromising the personal email accounts of numerous individuals, including customers of Corporate Victim #1; (3) exploiting a vulnerability in the website of Corporate Victim #2 to use it in their spamming activities; and (4) using the stolen PII as well as the compromised corporate computer networks and email accounts to send illegal spam on behalf of others for a fee.

Manner and Means of the Conspiracy

26. It was part of the conspiracy that, at defendant LIVINGSTON's direction, defendant CHMIELARZ wrote computer programs to: (1) steal confidential business information, including PII, from the computer servers of certain of the Corporate Victims; (2) access the email accounts of Corporate Victim #1's customers; (3) take control of the email servers of certain of the Corporate Victims, including Corporate Victim #2; and (4) send spam in a manner that would conceal the true origin of the email and bypass spam filters.

27. It was further part of the conspiracy that the conspirators used a variety of techniques, including proxy servers, botnets, and fake identities, to avoid detection, conceal their identities, and evade spam filters and similar anti-spam software.

28. It was further part of the conspiracy that defendant McARTHUR, who was employed by Corporate Victim #4, installed a remote administration tool on a computer with access to Corporate Victim #4's network without

authorization from Corporate Victim #4, and then provided access to Corporate Victim #4's network to defendants LIVINGSTON and CHMIELARZ for the purpose of stealing confidential business information, including the PII of millions of individual victims.

29. It was further part of the conspiracy that the conspirators sent unlawful spam messages using stolen PII and email servers of certain of the Corporate Victims and the email accounts of Corporate Victim #1's customers.

Overt Acts

30. In furtherance of the conspiracy and to effect its unlawful objects, defendant LIVINGSTON, defendant CHMIELARZ, defendant McARTHUR, and others committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

a. On or about September 19, 2012, defendant LIVINGSTON initiated, via an online payment system, a transfer of approximately $1,500 to defendant CHMIELARZ, who logged into his account from an IP Address in New Jersey on that same date.

b. On or about October 24, 2012, defendant LIVINGSTON sent defendant CHMIELARZ an online message containing the username and password for several email accounts hosted by Corporate Victim #1.

c. On or about March 15, 2013, defendant LIVINGSTON initiated, via an online payment system, a transfer of approximately $250 to defendant CHMIELARZ, who logged into his account from an IP Address in New

Jersey on that same date.

d. On or about May 10, 2013, defendant LIVINGSTON sent defendant CHMIELARZ an online message stating that a database they were stealing from Corporate Victim #3 contained records for approximately 10 million individuals.

e. On or about May 10, 2013, defendant LIVINGSTON initiated, via an online payment system, a transfer of approximately $400 to defendant CHMIELARZ.

f. On or about August 15, 2014, defendant McARTHUR provided defendants LIVINGSTON and CHMIELARZ access to Corporate Victim #4's computer network using a remote administration tool.

g. On or about August 15, 2014, defendant LIVINGSTON sent defendant CHMIELARZ an online message in which he estimated that Corporate Victim #4's database contained records for approximately 50 million individuals.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO
(Conspiracy to Commit Wire Fraud)

1. The allegations contained in paragraphs 1 through 23 of Count One of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From at least as early as in or about January 2012 through in or about July 2015, in Passaic County, in the District of New Jersey, and elsewhere, defendants

TIMOTHY LIVINGSTON,
a/k/a "Mark Loyd,"
TOMASZ CHMIELARZ, and
DEVIN McARTHUR

did knowingly and intentionally conspire and agree with each other and others to devise a scheme and artifice to defraud Corporate Victim #3, Corporate Victim #4, and others, and to obtain money and property, including the confidential business information of Corporate Victim #3, Corporate Victim #4, and others, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

Object of the Conspiracy

3. The object of the conspiracy was for defendant LIVINGSTON, defendant CHMIELARZ, defendant McARTHUR, and others to enrich themselves

by hacking into the computer networks of Corporate Victim #3 and Corporate Victim #4 to steal the confidential business information of Corporate Victim #3 and Corporate Victim #4, including the PII of tens of millions of their customers.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that defendant LIVINGSTON, defendant CHMIELARZ, defendant McARTHUR, and others, employed the manner and means set forth in paragraphs 26 through 29 of Count One of this Indictment.

In violation of Title 18, United States Code, Sections 1349.

COUNT THREE
(Conspiracy to Commit Fraud and Related Activity in Connection with Electronic Mail)

1. The allegations contained in paragraphs 1 through 23 of Count One of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From at least as early as in or about January 2012 through in or about July 2015, in Passaic County, in the District of New Jersey, and elsewhere, defendants

TIMOTHY LIVINGSTON,
a/k/a "Mark Loyd," and
TOMASZ CHMIELARZ

did knowingly and intentionally conspire and agree with each other and others to commit offenses against the United States, namely, to knowingly access a protected computer without authorization, and intentionally initiate the transmission of multiple commercial electronic mail messages from and through such computer; to knowingly use a protected computer to relay and retransmit multiple commercial electronic mail messages, with the intent to deceive and mislead recipients, and any Internet access service, as to the origin of such messages; and to knowingly materially falsify header information in multiple commercial electronic mail messages and intentionally initiate the transmission of such messages; and to knowingly register, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts, and two or more domain names, and

intentionally initiate the transmission of multiple commercial electronic mail messages from any combination of such accounts and domain names, contrary to Title 18, United States Code, Sections 1037(a)(1), 1037(a)(2), 1037(a)(3), 1037(a)(4), and 1037(b)(2).

Object of the Conspiracy

3. The object of the conspiracy was for defendant LIVINGSTON, defendant CHMIELARZ, defendant McARTHUR, and others to enrich themselves by: (1) compromising the personal email accounts of numerous individuals, including customers of Corporate Victim #1; (2) exploiting a vulnerability in the website of Corporate Victim #2 to use it in their spamming activities; (3) using the stolen PII in conjunction with compromised corporate computer networks and email accounts to send illegal spam on behalf of others for a fee; and (4) employing practices that obscured the true source of the spam emails being sent.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that defendant LIVINGSTON, defendant CHMIELARZ, defendant McARTHUR, and others, employed the manner and means set forth in paragraphs 26 through 29 of Count One of this Indictment.

Overt Acts

5. In furtherance of the conspiracy and to effect its unlawful objects, defendant LIVINGSTON, defendant CHMIELARZ, defendant McARTHUR, and others committed and caused to be committed the overt acts referenced in paragraph 30 of Count One of this Indictment.

In violation of Title 18, United States Code, Section 371.

FORFEITURE ALLEGATION AS TO COUNT ONE

1. Upon conviction of the offense of conspiracy to commit computer fraud, contrary to 18 U.S.C. § 1030, in violation of 18 U.S.C. § 371, as charged in Count One of this Indictment, defendants

TIMOTHY LIVINGSTON,
a/k/a "Mark Loyd,"
TOMASZ CHMIELARZ, and
DEVIN McARTHUR

shall forfeit to the United States:

a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such conspiracy offense; and

b. pursuant to 18 U.S.C. § 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such conspiracy offense.

2. The property subject to forfeiture includes, but is not limited to, a sum of money representing the amount of proceeds obtained as a result of the conspiracy offense charged in Count One, for which the defendants are jointly and severally liable; and all right, title, and interest of the defendants in the following property:

a. approximately $70,387.99 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]9855, held in the name of Timothy Livingston;

b. approximately $76,915.48 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]9783, held in the name of A Whole Lot of Nothing, LLC;

c. approximately $4,802.40 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]4593, held in the name of A Whole Lot of Nothing, LLC;

d. approximately $147,547.93 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]6185, held in the name of Timothy Livingston; and

e. one 2006 Ferrari F430 two-door Spider Convertible, VIN ZFFEW59A660144921, seized on or about July 27, 2015 in Fort Lauderdale, Florida;

f. the contents of Scottrade Account # [redacted]8422 held in the name of Timothy Livingston; and

g. one 2009 Cadillac Escalade SUV, VIN: 1GYFC23299R215132.

FORFEITURE ALLEGATION AS TO COUNT TWO

1. Upon conviction of the offense of conspiracy to commit wire fraud, contrary to 18 U.S.C. § 1343, in violation of 18 U.S.C. § 1349, as charged in Count Two of this Indictment, defendants

TIMOTHY LIVINGSTON,
a/k/a, "Mark Loyd,"
TOMASZ CHMIELARZ, and
DEVIN McARTHUR

shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the said conspiracy offense, and all property traceable thereto.

2. The property subject to forfeiture includes, but is not limited to, a sum of money representing the amount of proceeds obtained as a result of the conspiracy offense charged in Count Two, for which the defendants are jointly and severally liable; and all right, title and interest of the defendants in the following property:

a. approximately $70,387.99 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]9855, held in the name of Timothy Livingston;

b. approximately $76,915.48 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]9783, held in the name of A Whole Lot of Nothing, LLC;

c. approximately $4,802.40 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]4593, held in the name of A Whole Lot of Nothing, LLC;

d. approximately $147,547.93 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]6185, held in the name of Timothy Livingston;

e. one 2006 Ferrari F430 two-door Spider Convertible, VIN ZFFEW59A660144921, seized on or about July 27, 2015 in Fort Lauderdale, Florida;

f. the contents of the contents of Scottrade Account # [redacted]8422 held in the name of Timothy Livingston; and

g. one 2009 Cadillac Escalade SUV, VIN: 1GYFC23299R215132.

FORFEITURE ALLEGATION AS TO COUNT THREE

1. Upon conviction of the offense of conspiracy to commit fraud and related activity in connection with electronic mail, contrary to 18 U.S.C. § 1037, in violation of 18 U.S.C. § 371, as charged in Count Three of this Indictment, defendants

TIMOTHY LIVINGSTON,
a/k/a, "Mark Loyd," and
TOMASZ CHMIELARZ

shall forfeit to the United States, pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 1037(c) and 28 U.S.C. § 2461(c):

a. any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

b. equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

2. The property subject to forfeiture includes, but is not limited to, a sum of money representing the amount of proceeds obtained as a result of the conspiracy offense charged in Count Three, for which the defendants are jointly and severally liable; and all right, title and interest of the defendants in the following property:

a. approximately $70,387.99 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]9855, held in the name of Timothy Livingston;

b. approximately $76,915.48 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]9783, held in the name of A Whole Lot of Nothing, LLC;

c. approximately $4,802.40 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]4593, held in the name of A Whole Lot of Nothing, LLC;

d. approximately $147,547.93 seized on or about July 27, 2015 from Wells Fargo Bank Account No. [redacted]6185, held in the name of Timothy Livingston; and

e. one 2006 Ferrari F430 two-door Spider Convertible, VIN ZFFEW59A660144921, seized on or about July 27, 2015 in Fort Lauderdale, Florida;

f. the contents of Scottrade Account # [redacted]8422 held in the name of Timothy Livingston; and

g. one 2009 Cadillac Escalade SUV, VIN: 1GYFC23299R215132.

SUBSTITUTE ASSETS PROVISION
(Applicable to All Forfeiture Allegations)

1. If any of the property described above, as a result of any act or omission of the defendant(s):

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. §§ 982(b), 1030(i) and 1037(c)(2), and 28 U.S.C. § 2461(c), to forfeiture of any other property of the defendant(s) up to the value of the above-described forfeitable property.

A TRUE BILL

FOREPERSON

Paul J. Fishman | Lmc

PAUL J. FISHMAN
UNITED STATES ATTORNEY

CASE NUMBER: 15-626 (WJM)

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

TIMOTHY LIVINGSTON,
a/k/a "Mark Loyd,"
TOMASZ CHMIELARZ, and
DEVIN McARTHUR

INDICTMENT FOR
18 U.S.C. § 371
18 U.S.C. § 1349

[redacted]

Foreperson

PAUL J. FISHMAN
U.S. ATTORNEY
NEWARK, NEW JERSEY

DANIEL SHAPIRO
ASSISTANT U.S. ATTORNEY
(973) 353-6087

USA-48AD 8
(Ed. 1/97)

CLERK
U.S. DISTRICT COURT
DISTRICT OF NEW JERSEY
RECEIVED
2015 DEC 11 P 5:13